

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Mateus Bruno Araújo

***Personal Blockchain: Uma Estratégia de Gerenciamento de
Consentimento de Dados Pessoais Dirigida ao Usuário***

Fortaleza – CE

3 de maio de 2023

Mateus Bruno Araújo

***Personal Blockchain: Uma Estratégia de Gerenciamento
de Consentimento de Dados Pessoais Dirigida ao Usuário***

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia do Ceará, como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Linha de Pesquisa: Sistemas Distribuídos

Orientador: Prof. Dr. Cidcley Teixeira de Souza

Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (PRPI)

Programa de Pós-Graduação em Ciência da Computação (PPGCC)

Fortaleza – CE

3 de maio de 2023

Dados Internacionais de Catalogação na Publicação
Instituto Federal do Ceará - IFCE
Sistema de Bibliotecas - SIBI
Ficha catalográfica elaborada pelo SIBI/IFCE, com os dados fornecidos pelo(a) autor(a)

ARAÚJO, MATEUS.

Personal Blockchain: Uma Estratégia de Gerenciamento de Consentimento de Dados Pessoais Dirigida ao Usuário / MATEUS ARAÚJO. - 2023.
57 f. : il. color.

Dissertação (Mestrado) - Instituto Federal do Ceará, Mestrado em Ciência da Computação, Campus Fortaleza, 2023.

Orientação: Prof. Dr. Cidcley Teixeira de Souza.

1. blockchain. 2. GDPR. 3. LGPD. 4. gerenciamento de consentimento. I. Título.

CDD 004



Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)
Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (PRPI)
Programa de Pós-Graduação em Ciência da Computação (PPGCC)

Mateus Bruno Araújo

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, sendo aprovada pela Coordenação do Programa de Pós-Graduação em Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia do Ceará e pela banca examinadora:

Orientador: Prof. Dr. Cidcley Teixeira de Souza
Instituto Federal de Educação, Ciência e Tecnologia do
Ceará (IFCE)

Prof. Dr. Atslands Rego da Rocha
Universidade Federal do Ceará (UFC)

Prof. Dr. Antonio Wendell de Oliveira Rodrigues
Instituto Federal de Educação, Ciência e Tecnologia do
Ceará (IFCE)

Fortaleza – CE
3 de maio de 2023

Este trabalho é dedicado aos meus pais, meus primeiros professores na vida, e à todos os professores, tutores e colegas que me ajudaram em todas as minhas conquistas acadêmicas.

Agradecimentos

A Deus, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho. Ao meu orientador, Prof. Cidcley Teixeira de Souza, pelo apoio, dedicação e por sempre acreditar em mim e no projeto.

Também agradeço aos meus pais que sempre me apoiaram e me deram condições de poder chegar onde cheguei. A minha esposa por sempre está ao meu lado me apoiando e me dando força para nunca desistir de meus sonhos.

E por fim, mas não menos importantes, às pessoas em quem convivi a longo desses anos de curso, que me incentivaram e que certamente tiveram impacto na minha formação acadêmica.

“O homem mais pobre desafia em sua casa todas as forças da Coroa, sua cabana pode ser muito frágil, seu teto pode tremer, o vento pode soprar entre as portas mal ajustadas, a tormenta pode nela penetrar, mas o Rei da Inglaterra não pode nela entrar.”
(Lord Chatan)

Resumo

Com a entrada em vigor na União Europeia da *General Data Protection Regulation* (GDPR), em maio de 2018, houve a necessidade de todos os sistemas se adequarem ao rol de princípios da nova lei. O mesmo processo legislativo está ocorrendo no Brasil, com a LGPD (Lei Geral de Proteção a Dados), que entrou em vigor em setembro de 2020. O princípio do gerenciamento de consentimento se destaca do rol de princípios das duas legislações. Sendo ele necessário para fornecer mais controle aos usuários sobre seus dados. O usuário, após a adequação dos sistemas à lei, poderá consentir sobre o processamento e armazenagem dos seus dados. Entretanto, as tecnologias atuais para realizar o gerenciamento desses dados não oferecem aos titulares dos dados a real posse dos mesmos, ficando a cargo dos requisitantes a execução de todas as operações sobre esses dados. Neste trabalho é proposta uma nova estratégia para o gerenciamento de consentimento, a *Personal Blockchain*. Além do desenvolvimento de um modelo arquitetural para possibilitar a implementação da *Personal Blockchain*, a *blockchain* matricial com âncora. A nova estratégia tem o intuito de possibilitar o maior empoderamento do usuário na gestão dos seus dados como preconizada pelas leis de proteção de dados pelo mundo.

Palavras-chave: *blockchain*. GDPR. LGPD. gerenciamento de consentimento.

Abstract

With the entry into force in the European Union of the *General Data Protection Regulation* (GDPR), in May 2018, there was a need for all systems to adapt to the list of principles of the new law. The same legislative process is taking place in Brazil, with the LGPD (General Data Protection Law), which came into force in September 2020. The principle of consent management stands out from the list of principles of both legislations. It is needed to provide users with more control over their data. The user, after adapting the systems to the law, may consent to the processing and storage of his data. However, the current technologies for managing this data do not offer the data holders real possession of the same, leaving it to the requesters to carry out all operations on the data. In this work, a new strategy for managing consent to *Personal Blockchain* is proposed. In addition to the development of a new architectural model to enable the implementation of *Personal Blockchain*, a new distributed system architecture. The new strategy is intended to enable greater user empowerment in the management of their data as recommended by data protection laws around the world.

Keywords: blockchain. GDPR. LGPD. consent management.

Lista de ilustrações

Figura 1 – Diagrama de estados.	37
Figura 2 – Representação de uma <i>blockchain</i> matricial	38
Figura 3 – Arquitetura física de comunicação.	41
Figura 4 – Diagrama de sequência de concessão do consentimento e atualização de dados.	43
Figura 5 – Diagrama de sequência de concessão da remoção e revogação.	44
Figura 6 – Gráfico da distribuição de blocos por tempo de inserção na <i>blockchain</i> matricial com âncora no teste de 30.000 blocos com dificuldade de 5 zeros.	49
Figura 7 – Gráfico da distribuição de blocos por tempo de inserção na <i>blockchain</i> tradicional no teste de 30.000 blocos com dificuldade de 5 zeros.	49

Lista de tabelas

Tabela 1 – Tabela de benchmark de execuções de inserção em massa.	47
---	----

Lista de Algoritmos

- 1 Algoritmo de criação de blocos da *blockchain* matricial com âncora. . . . 40

Sumário

1	INTRODUÇÃO	23
1.1	Motivação para a Dissertação	24
1.2	Descrição do Problema	25
1.3	Objetivos Geral e Específicos	26
1.4	Estrutura da Dissertação	26
2	FUNDAMENTAÇÃO TEÓRICA	29
2.1	GDPR e LGPD	29
2.1.1	Princípio de Consentimento	29
2.1.2	Direito de Esquecimento	30
2.1.3	Direito a Retificação	30
2.1.4	Minificação de Dados	31
2.2	Blockchain e Leis de Proteção	31
2.3	<i>Blockchain</i> de Rede Individual	32
2.3.1	Ataque de Consenso e Solução	32
2.3.2	Recriação da <i>blockchain</i> e Solução	32
3	TRABALHOS RELACIONADOS	35
4	<i>PERSONAL BLOCKCHAIN</i>	37
4.1	Arquitetura da <i>Blockchain</i> Matricial com Âncora	38
4.1.1	<i>Blockchain</i> Interna ou Matricial	38
4.1.2	<i>Blockchain</i> Externa ou Âncora	39
4.1.3	Modelo Estrutural Interno	40
4.1.4	Contratos de Serviços	40
5	CENÁRIOS DE USO	43
5.1	Caso exemplo: Concessão de dados	44
5.2	Caso exemplo: Retificação de dados	44
5.3	Caso Exemplo: Solicitação de Esquecimento	45
5.4	Caso Exemplo: Auditoria	45
6	BENCHMARK E COMPARAÇÃO	47
7	CONCLUSÃO	51

REFERÊNCIAS	53
-----------------------	----

1 Introdução

Cada vez mais, os marcos legais sobre proteção de dados estão em destaque pelo mundo. Eles têm como objetivo dar poder aos usuários de decidir sobre seus dados, tendo como um dos principais marcos regulatórios desse tema a GDPR (General Data Protection Regulation) (VOIGT; BUSSCHE, 2017). Do ponto de vista dessa legislação, o consentimento deve ser fornecido de modo explícito, específico e entregue de vontade própria e deve existir um propósito específico para a captura desses dados.

O artigo 7º da GDPR enfatiza as condições de consentimento: o usuário tem o direito de dar e retirar o consentimento de forma livre e informada (SIM; CHUA; TAHIR, 2019), (LEE et al., 2019). Sendo assim, os dados dos usuários não podem ser armazenados e processados sem o seu consentimento. Análoga a lei europeia outros códigos como o *Fair Credit Reporting Act* (FCRA), nos Estados Unidos; e a Lei Geral de Proteção de Dados (LGPD), no Brasil, também exigem o consentimento para o processamento e armazenamento do dado (AL-ZABEN et al., 2018), (HAQUE et al., 2021).

Podem ser destacados quatro atores no processo de gerenciamento de concessão:

- o Usuário, dono ou gerador dos dados;
- o Controlador, pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018), equivalente ao Responsável na GDPR;
- o Operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018), equivale ao Processador da GDPR; e
- o Encarregado, ou DPO (*Data Protection Officer*) na GDPR, pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (BRASIL, 2018), ou seja, o ente que atua entre o órgão fiscalizador e a controladora.

De maneira simplificada, pode-se dizer que o usuário, o gerador do dado, deseja usar um serviço de uma empresa, porém para utilizar esse serviço é necessário que o usuário conceda o registro de alguns de seus dados à empresa. Ao realizar essa concessão, a empresa é caracterizada como um controlador. Caso seja necessário, para a empresa realizar o serviço requerido pelo usuário, compartilhar dados do usuários com outras empresas, essas empresas terceirizadas seriam consideradas operadores ou processadores. Além desses atores, também existe a entidade que regula esse processo, chamada acima de encarregado.

Adicionalmente ao surgimento de códigos legais das leis de proteção de dados, surge

a necessidade de adequação dos sistemas e das tecnologias. Os marcos regulatórios impõem mudanças, a visão passa ser de quem deu causa de existência do dado, o dono do dado, como versa o artigo 1º da GDPR (PARLIAMENT, 2016). A partir desse momento o dono do dado deve permitir ou não o armazenamento e processamento do dado.

Uma das tecnologias que vem sendo amplamente utilizada nos últimos anos para empoderar os seus usuários, dando um controle maior sobre suas transações e retirando a necessidade de existir um intermediário é o *blockchain*. Tendo como algumas de suas características principais a transparência, a independência e a auditabilidade. Pontos importantes para os normativos de proteção de dados (AHMED et al., 2020).

Porém, de acordo com Saglam et al. (2020), muitos sistemas baseados em *blockchain* não apresentam adequação à GDPR, sendo que menos que a metade dos sistemas analisados tinha algum tipo de informação sobre a lei. De acordo com o relatório do Observatory e Forum (2018), os princípios incorporados pela lei são paradoxos a alguns pontos da tecnologia *blockchain*, como o direito ao consentimento.

Nesse cenário, cada vez mais se faz necessário a criação de uma estratégia para não só adequar sistemas baseados em *blockchain* às novas legislações, como também utilizar seus pontos fortes no empoderamento do usuário na gerência sobre seus dados. Esse trabalho apresenta o desenvolvimento de uma estratégia para permitir o gerenciamento de dados pessoais pelo próprio usuário, baseada em *blockchain*, que possibilita o controle da distribuição dessas informações, além de permitir que tanto os usuários como os solicitantes dessas informações possam garantir quando, para quem e com que finalidade foi dado permissão para processamento e armazenamento dos dados. Essa estratégia é a *Personal Blockchain*, uma nova forma de armazenar e compartilhar dados voltado para o usuário e aderente aos direitos de consentimento, de esquecimento, de retificação e minificação dos dados. Porém, para implementá-la, foi necessário o desenvolvimento de uma arquitetura, a *blockchain* de rede individual com âncora.

Além da arquitetura, também foi necessário, para implementar a *Personal Blockchain*, expandir a topologia linear das *blockchains* tradicionais, criando assim uma topologia interna chamada de *blockchain* matricial ou bi-dimenssional. Nesse trabalho não foram abordados temas relativos a estrutura de segurança da *Personal Blockchain*, mas está previsto em trabalhos futuros no capítulo de conclusão.

1.1 Motivação para a Dissertação

Como é sabido, a tecnologia tem de acompanhar as inovações legais, desse modo, fornecer estratégias para dar suporte às implementações das questões relacionadas às novas legislações de proteção de dados tem se tornado cada vez mais evidente no âmbito das organizações. Contudo, o que se pode observar é que os sistemas atuais ainda estão

dirigidos aos controladores de dados, não aos donos dos dados. Para realizar qualquer modificação nos dados é necessária uma solicitação ao controlador, que é quem efetivamente fará a mudança dos dados. Se o controlador, por algum motivo, não estiver disponível no momento, o usuário que terá que buscar uma forma contatá-lo.

Nesse cenário, é apresentado nessa pesquisa a criação de uma estratégia para possibilitar o empoderamento do usuários frente ao controlador, possibilitando o usuário ter a guarda de seus dados e invertendo a lógica do processo de obtenção de dados, a *Personal Blockchain*. Para apoiar a solução foi desenvolvida uma arquitetura de estrutura de dados baseado em *blockchain*, a *blockchain* de rede individual com âncora, que também pode ser chamada de *blockchain* matricial com âncora, por ser baseada em uma nova topologia de *blockchain* apresentada no projeto chamada de *blockchain* matricial.

Dessa forma, o uso da *blockchain* foi motivado por suas características intrínsecas como a auditabilidade e imutabilidade. Corroborando com o uso do *blockchain*, também foi considerado o crescente interesse da academia pelo tema, como podemos ver em Al-Zaben (AL-ZABEN et al., 2018), Belen Saglam (SAGLAM et al., 2020), Herian (HERIAN, 2020), Huang (HUANG; YEH; HUANG, 2019) e Sim (SIM; CHUA; TAHIR, 2019). Entretanto, a *blockchain* é considerado incompatível com alguns direitos preconizados pelas leis de proteção de dados como o direito de consentimento e seus corolários, os direitos de reificação e de esquecimento (artigo 17º e 5º da GDPR). O direito de consentimento abrange a possibilidade de o dono dos dados gerenciá-los permitindo, revogando ou retificando seus dados. Assim, sendo a *blockchain* considerada imutável, uma vez que as informações são registradas na *blockchain* não podem ser removidas ou editadas, deixando claro o conflito com o espírito legal da GDPR (CASINO et al., 2020).

Deste modo, é evidente que as arquiteturas tradicionais baseadas em *blockchain* apresentam conflitos com as leis de proteção. Assim, para viabilizar a *Personal Blockchain* foi necessário o desenvolvimento de uma arquitetura para *blockchains*, a *blockchain* de rede individual com âncora, que visa possibilitar a criação de *blockchains* de cadeias curtas que são ancoradas criptograficamente em uma *blockchain* pública de cadeia longa. Dessa forma, mitigando as limitações dessa tecnologia para o gerenciamento de consentimento indicadas na literatura podem ser suplantadas.

1.2 Descrição do Problema

O consentimento pode ser obtido de uma variedade de formas, aplicativos móveis, sistemas de CRM (*Customer Relationship Management*), plataformas de marketing, centros de contato e pontos de vendas, dentre outros. A forma tradicional de obter consentimento é através dos termos de condições presentes em quase todos os sites da web e armazenados juntos ao solicitante da informação (KAKARLAPUDI; MAHMOUD, 2021). Por exemplo,

um paciente pode desejar compartilhar seus dados com um médico, mas não deseja compartilhar seus dados com um pesquisador. Nesse cenário, o usuário deu consentimento parcial para compartilhar seus dados.

Com a introdução do GDPR (Regulamento Geral de Proteção de Dados) e outras leis de privacidade em vários países, as empresas devem garantir que o usuário esteja totalmente ciente do consentimento que estão dando. A empresa deve fornecer informações precisas sobre as situações em que seus dados serão utilizados; em outras palavras, deve haver transparência do processamento e gerenciamento dos dados.

Existem algumas soluções baseadas em *blockchain* para o problema de obtenção, armazenamento e gerenciamento de consentimento. Mas nenhuma delas traz a possibilidade de o usuário ter seus dados guardados em sua própria infraestrutura, ou seja, em seu próprio domínio. Nos métodos apresentados, os dados estão sob a custódia de um grupo de controladores ou de apenas um controlador. Analisando as revisões bibliográficas de Haque et al. (2021), Lee et al. (2019), Kakarlapudi e Mahmoud (2021), não é encontrado alguma solução para possibilitar o controle dos dados realizado diretamente pelo dono e baseado em *blockchain*.

A arquitetura proposta aqui tem como intuito possibilitar que a guarda, remoção e modificação dos dados seja feita diretamente pelos meios do usuário, sem necessitar de aprovação ou ação previa dos controladores, apenas a eles compete, se necessário a propagação para seus registros dos dados.

1.3 Objetivos Geral e Específicos

O objetivo principal do trabalho é definir e explorar a nova arquitetura de referência proposta, a *Personal Blockchain*. A *Personal Blockchain* visa possibilitar o armazenamento, compartilhamento, e gerenciamento do consentimento de dados gerados pelo usuário. Essa arquitetura trará empoderamento ao usuário frente o solicitante das informações. A exploração será realizada a partir da arquitetura de solução, também desenvolvida nesse trabalho, a *blockchain* matricial com âncora, uma arquitetura baseada na *Personal Blockchain*. Essa arquitetura será avaliada comparativamente com arquiteturas tradicionais para identificar seus gargalos e pontos positivos, assim, possibilitando a observação da estratégia proposta em relação às já existentes.

1.4 Estrutura da Dissertação

O trabalho seguirá com as seguintes partes: fundamentação teórica, apresenta os principais temas abordados pelo projeto; motivação e solução, mostra o porquê da arquitetura; trabalhos relacionados, apresenta o estado da arte sobre a utilização de *blockchain*

com o gerenciamento de consentimento e compara com a arquitetura proposta; *Personal Blockchain*, apresentação do conceito da *Personal Blockchain* e suas características; cenários de uso, apresenta cenários de uso com a *Personal Blockchain*; *benchmark* e comparação, traz os *benchmarks* e comparações sobre a arquitetura proposta e as arquiteturas tradicionais das *blockchains*; e a conclusão do trabalho.

2 Fundamentação Teórica

2.1 GDPR e LGPD

GDPR e a LGPD são duas das principais leis de proteção e privacidade de dados na Europa e no Brasil, respectivamente. Chamadas de leis de proteção de dados, elas normatizam sobre como os dados devem ser usados e guardados; e quais as responsabilidades dos envolvidos sobre sua guarda e processamento. Pode-se dizer que as leis de proteção de dados têm como um de seus propósitos empoderar os usuários, geradores dos dados, dando a possibilidade de terem o máximo de gerência possível sobre os seus dados (TATAR; GOKCE; NUSSBAUM, 2020), (BRASIL, 2018), (PARLIAMENT, 2016).

Não só no Brasil ou na Europa que o tema vem sendo amplamente discutido e normatizado. Cada vez mais códigos jurídicos sobre o tema estão sendo promulgados em todo o mundo. A urgência no tema se dá a partir da explosão da coleta de dados dos usuários. Principalmente, pois, muitas vezes, essa coleta de dados está sendo usada de uma forma desregrada e antiética.

Em síntese, as leis de proteção de dados consagram a capacidade de aceitar ou não a coleta e processamento dos dados do usuário, consequentemente possibilitando a capacidade de consentir ou não a permanência dos dados com o solicitante e, também, dando um maior controle sobre os dados ao usuário que os gerou. No entanto, as novas legislações entram em conflito com alguns modelos tecnológicos, tecnologias e ferramentas utilizadas no mundo atual. Quando isso ocorre, os modelos devem evoluir e se adequar as novas legislações (TATAR; GOKCE; NUSSBAUM, 2020).

No trabalho, será abordado apenas quatro princípios encontrados na GDPR e na LGPD: o princípio do consentimento e seus corolários, o direito do esquecimento e da retificação; e o princípio da minimização do processamento dos dados (HJERPPE; RUOHONEN; LEPPÄNEN, 2020).

2.1.1 Princípio de Consentimento

A noção de consentimento foi estudada em várias disciplinas, medicina, direito e filosofia entre outras. O consentimento é um conceito baseado fortemente no princípio da autonomia. O consentimento é a permissão ou acordo realizado pelo titular de algo para que outrem realize ações ou tome conhecimento sobre o algo. As leis de proteção de dados estenderam a noção de consentimento ao contexto digital, ou seja, o consentimento deve ser dado aos termos de serviço de um site que deseja coletar e processar os dados pessoais dos usuários, assim o titular dos dados reconhece que foi suficientemente informado sobre

para quê e por quem os dados estão sendo usados. O principal objetivo de promover o princípio do consentimento é fornecer transparência e propiciar mais controle sobre os dados pessoais ao titular dos dados (AHMED et al., 2020).

A GDPR e a LGPD visam tornar o entendimento para consentimento mais inequívoco e explícito possível. Portanto, o consentimento é uma noção importante online, uma vez que se baseia na ideia de que os usuários individuais das redes online devem fazer escolhas conscientes, racionais e autônomas sobre a divulgação de seus dados pessoais. No artigo 5º, inciso XII, a LGPD e no artigo 7º da GDPR definem que o consentimento é uma manifestação livre, informada e inequívoca pela qual o titular dos dados concorda com o tratamento de seus dados pessoais para a finalidade informada (BRASIL, 2018), (PARLIAMENT, 2016). A partir do princípio do consentimento, ou direito ao consentimento, decorrem outros dois princípios: o direito ao esquecimento e o direito à reificação.

2.1.2 Direito de Esquecimento

O direito ao esquecimento tem suas raízes na decisão proferida em 2014 pelo Tribunal de Justiça da União Europeia em um caso movido contra a Google Inc. na Espanha (AEPD, 2014). O artigo 17 do GDPR, que estabelece o direito de apagamento, codifica principalmente a conclusão do tribunal de que o consentimento deve ser retirado tão facilmente quanto é concedido. Consequentemente, os dados pessoais devem ser apagados imediatamente quando o controlador de dados não tiver mais base legal para retê-los ou processá-los. Em outras palavras, o titular dos dados tem o direito de que seus dados pessoais sejam apagados quando estiverem sob a custódia de outra pessoa, sem qualquer justificativa.

Tal direito também é apresentado na lei brasileira, o artigo 18 da LGPD exhibe diversos itens que corroboram com o texto da lei de proteção de dados europeia, inclusive em seu item IX traz: “IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.” (BRASIL, 2018).

Em particular, o titular dos dados deve ter o direito de que seus dados pessoais sejam apagados e deixem de ser processados quando os dados pessoais não forem mais necessários em relação aos fins para os quais são coletados ou de outra forma processados, caso o titular dos dados tenha se retirado o seu consentimento ou objeções ao tratamento de dados pessoais que lhe digam respeito, ou quando o tratamento dos seus dados pessoais não esteja de acordo com os regulamentos pátrios.

2.1.3 Direito a Retificação

O artigo 18 da LGPD traz uma sequência de itens que explicitam o princípio do Direito de Retificação. No caput do artigo traz: “O titular dos dados pessoais tem direito a

obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:” (BRASIL, 2018) um rol exaustivo, o qual pode ser destacado o item “III - correção de dados incompletos, inexatos ou desatualizados;”(BRASIL, 2018). Também podemos encontrar referência a esse direito na lei europeia, quando afirma que o titular dos dados deve ter direito à retificação dos dados pessoais que lhe dizem respeito (PARLIAMENT, 2016).

2.1.4 Minificação de Dados

A minificação de dados está associada ao compartilhamento mínimo dos dados armazenados e seu uso. Quanto menos controladores e processadores de dados houver, menor o risco de utilização indevida dos dados. Tal princípio se alinha ao princípio do consentimento, quando se coloca que a autorização do consentimento tem de ser dada de forma inequívoca ao controlador e processador dos dados e que esse é responsável legal sobre a manipulação desses dados pelos seus parceiros.

2.2 Blockchain e Leis de Proteção

A *blockchain* é um livro razão digital de transações submetidas a rede *blockchain* (STAN; MICLEA, 2019), que registra transações de forma segura, transparente, resistente a adulteração e distribuída. A *blockchain* é a tecnologia subjacente do *Bitcoin* e outras criptomoedas. Se tornou amplamente conhecida após a introdução do *Bitcoin* em 2009 (NAKAMOTO, 2008). Hoje, a adoção da *blockchain* é muito mais ampla do que só criptomoedas (SANDHU; PABLOS, 2020).

Porém a *blockchain* traz diversos pontos de conflitos com as principais leis de proteção de dados, especialmente as já citadas. Levando em consideração a imutabilidade da cadeia *blockchain* e o grande volume de processadores (atores que processam os dados dos usuários) e armazenadores (atores que armazenam os dados dos usuários) possíveis, é um grande desafio possibilitar a exclusão e a retificação dos dados (LEE et al., 2019) e gerenciar a concessão de consentimento dos usuários, visto que, um consentimento é dado de forma clara e inequívoca para um ator específico (BRASIL, 2018), (PARLIAMENT, 2016).

Além dos conflitos já citados, Haque (HAQUE et al., 2021) faz um estudo bibliográfico sobre vários métodos para a retificação e remoção dos dados consentidos e em todos os métodos apresentados o usuário não é o foco da estratégia. A literatura traz um viés muito pautado pelo ponto de vista do requisitante, não do usuário. Após a autorização dada pelo dono dos dados, os dados passam a estar sob a guarda de outrem, sem a necessidade de um processo claro e padronizado e acessível ao usuário que garanta a irretratabilidade tanto de um lado como do outro da transação.

2.3 *Blockchain* de Rede Individual

Um outro ponto que foi matéria de estudo para o trabalho foi a possibilidade de *blockchains* de rede individual. A *Personal Blockchain*, por aderir ao direito de minificação do processo, tem como intenção minimizar o máximo o tráfego de informações entre atores da rede, sendo uma rede individual, com apenas um contributor, a situação mais favorável a esse princípio. Durante a pesquisa, não foram encontradas referências sobre redes de *blockchain* com apenas um ator. Visto esse gap na literatura, foi necessário identificar quais os principais problemas para esse tipo de uso de *blockchains* não ser amplamente utilizado. A seguir será apresentado os principais problemas encontrados para possibilitar a utilização de *blockchains* com apenas um ator.

2.3.1 Ataque de Consenso e Solução

Um ataque de consenso acontece quando um ator ou um grupo de atores se utilizam da maioria dos nós em uma regra de consenso para criar ou modificar dados de forma maliciosa (ANTONOPOULOS, 2017). Supondo uma regra de consenso onde a metade mais um de nós em uma rede seja considerado a maioria da rede, em um ataque de consenso, nessa rede, é necessário sequestrar ou obter a metade mais um dos nós para que seja possível “aprovar” qualquer registro na *blockchain* sem necessariamente ser um registro válido.

Como a *Personal Blockchain* tem como premissa a existência apenas de um ator na rede da *blockchain*, ou seja, esse ator sempre detém a maioria na regra de consenso. Caso queira, ele pode incluir ou retirar dados sem a necessidade de passar por crivo de outros. Porém, essa possibilidade abre uma vulnerabilidade: o usuário pode adulterar os dados e imputar ao cliente dos dados (a quem foi compartilhado os dados) o fato de que ele está utilizando informações inverídicas ou adulteradas.

Para solucionar o problema do ataque de consenso, foi utilizada uma estratégia de âncora externa (WEBER et al., 2019). Com a âncora as informações inseridas na carteira de dados são lastreadas em uma *blockchain* tradicional com vários outros participantes. Caso seja necessário, podem ser auditados todos os dados da carteira.

2.3.2 Recriação da *blockchain* e Solução

A segunda dificuldade encontrada foi a possibilidade de recriação da *blockchain* com utilização de colisões de hash. Teoricamente, as funções de criação de hash são injetoras, ou seja, a cada semente passada para a função é gerado um hash distinto. Entretanto, existem casos em que a função de hash gera uma colisão, isto é, gera o mesmo hash para entradas diferentes. O risco aumenta levando-se em consideração que todos os dados inseridos estão

no domínio de apenas um ator. Esse ator tendo poder computacional suficiente, é possível adulterar a estrutura da *blockchain* mesmo com a âncora.

Para mitigar o problema de uma recriação total ou parcial da cadeia, foi desenvolvido um modelo arquitetural bidimensional para a *blockchain*, denominada de *blockchain* matricial. Como pode ser visto na Figura 2, a *blockchain* matricial é estruturada acoplando blocos adicionais à estrutura padrão da *blockchain* tradicional. Todos os blocos são interdependentes, utilizam-se do conteúdo do bloco anterior para gerar seu hash, mitigando assim a possibilidade de recriação da cadeia, pois seria necessário colidir $2N$ hashes pelo menos, sendo N a ordem de entrada das informações na cadeia (ex: o quinto bloco de informação tem ordem 5).

3 Trabalhos Relacionados

A crescente procura pelo tema *blockchain* com direitos de proteção de dados é notório como pode ser visto em Haque (HAQUE et al., 2021) e em Huang (HUANG et al., 2021). Dentre os principais temas encontrados nas revisões bibliográficas, é possível encontrar: deleção, modificação de dados, gerenciamento de consentimento e minificação do processamento de dados, porém todos os artigos encontrados nas revisões focam no lado do cliente das informações, não no lado do dono dos dados. As soluções discutidas a seguir também focam no requerente dos dados, não foram encontradas soluções que tivessem como base a utilização da *blockchain* como estrutura principal de armazenamento de dados e com a guarda no lado do usuário, o dono dos dados.

Os termos deleção e modificação de dados são as expressões técnicas do direito de esquecimento e de retificação, dois dos princípios das leis de proteção de dados pelo mundo (KADENA; HOLICZA, 2018). Sobre esses princípios, Stan e Miclea (STAN; MICLEA, 2019) ressaltam a incompatibilidade entre eles e sistemas baseados em *blockchain*. Dentro do trabalho, é concluído que a única maneira do direito de deleção ou retificação ser possível com estruturas baseadas em *blockchain* é considerar que a exclusão de dados não significa necessariamente exclusão física, ou seja, a exclusão lógica ser considerada aderente aos princípios citados.

Nos casos de exclusão e modificação dos dados em um sistema baseado em *blockchain*, é possível considerar que a edição, nada mais é, que a substituição de um dado registro por outro (POLITOU et al., 2020). Em Kadena (KADENA; HOLICZA, 2018), é sugerido um algoritmo de consenso em uma *blockchain* que se deseja excluir dados. Há uma votação e a maioria aprovando, os dados podem ser removidos. Nesse caso, pode ocorrer outro problema: remover alguns blocos antigos e interromper a cadeia. Em contraste ao trabalho aqui proposto, toda a gestão dos dados está em uma única parte do processo, mesmo que seja utilizada uma estratégia distribuída, a solução de Kadena ainda apresentará problemas com o princípio da minificação do processamento de dados.

Uma outra solução para exclusão e retificação é o apresentado em Al-Zaben (AL-ZABEN et al., 2018). No trabalho, é proposto uma arquitetura *blockchain* com uma estrutura de dados *off-chain*, que usa um banco de dados local para preservar e armazenar os dados, assim, os dados sensíveis são armazenados dentro do banco de dados não da *blockchain*. Ao armazenar os dados fora da cadeia, o sistema estará em conformidade com o direito de esquecimento e retificação, uma vez que, os dados fora da cadeia podem ser excluídos ou alterados a qualquer tempo. Bayle também utilizou processo semelhante (BAYLE et al., 2018). Comparativamente à *Personal Blockchain*, é possível identificar

que todo o processo é executado por outrem, sendo que o dono dos dados solicita ações, o gerenciamento de fato dos dados é realizado pelo cliente dos dados, que nesse caso se comporta quase como um dono, visto que tem a guarda e controle dos dados.

Em Lee (LEE et al., 2019), é proposta uma *blockchain* customizável, que os usuários têm o direito de retirar o consentimento, assim sendo, solicitar a remoção dos dados. Nessa estrutura, os proprietários dos dados escolhem o nível de dificuldade de modificação de sua transação antes de enviá-la. Importante salientar que esse método utiliza uma estrutura *multichain*: uma única cadeia principal para a aprovação da transação e várias cadeias laterais para modificação da transação, ou seja, a arquitetura da solução é composta por diversas *blockchains*, uma principal e varias laterais para armazenar as informações dos usuários, sendo assim não é necessário modificar dados na cadeia principal. As modificações de transação são realizadas nas *sidechains*. Apresentam as mesmas diferenças ao trabalho proposto que Bayle e Al-Zaben.

Não menos importante, a literatura também aborda muito sobre as questões do gerenciamento de consentimento e revogação de acesso aos dados, como pode ser visto em Al-Zaben (AL-ZABEN et al., 2018), Belen Saglam (SAGLAM et al., 2020), Herian (HERIAN, 2020), Huang (HUANG; YEH; HUANG, 2019) e Sim (SIM; CHUA; TAHIR, 2019). As abordagens trazem pequenos sistemas e utilizam *smart contracts* para viabilizar o gerenciamento de consentimento e revogação de acesso. Quando retirado o consentimento, e conseqüente exclusão dos dados, é utilizada estratégias similares as já comentadas. Entretanto, a utilização de contratos inteligentes, quando usados em sistemas distribuídos e públicos, não é aderente ao princípio da minificação dos processadores e dos consumidores, assim como dificulta a aderência ao princípio do consentimento, visto a dificuldade em identificar todos os possível processadores e detentores de dados. Quando utilizado em um sistema interno, com apenas uma parte sendo detentora do sistema, este sistema estará sob o controle do cliente dos dados, o dono dados apenas exercerá um poder parcial. O gerenciamento do ciclo de vida dos dados será do cliente dos dados.

Em toda a bibliografia apresentada, não foi encontrado nenhuma arquitetura com intuito similar de possibilitar uma *blockchain* de rede individual, ou seja, com apenas um ator na rede. Também, não foi encontrado um arquitetura de registro de dados focado no gerador dos dados no contexto das leis de proteção de dados. Sendo assim não foi possível realizar comparações diretas entre soluções já existente e a proposta.

4 *Personal Blockchain*

A *Personal Blockchain* é a nova estratégia que visa a aderência aos princípios de consentimento, de esquecimento, de retificação e de minificação do processamento de dados. Seu principal objetivo é empoderar os seus usuários com a capacidade de gestão direta sobre seus dados. O conceito apresentado traz uma forma de possibilitar o gerenciamento dos dados, incluindo seu compartilhamento e revogação de acesso. Também, traz a capacidade de registrar todos os eventos do ciclo de vida dos dados, dotando arquiteturas baseadas nele características como a irretratabilidade do evento, confidencialidade e integridade dos dados. Contudo, dependendo da implementação da *Personal Blockchain* e do ambiente de implantação, pode-se agregar outras características de segurança.

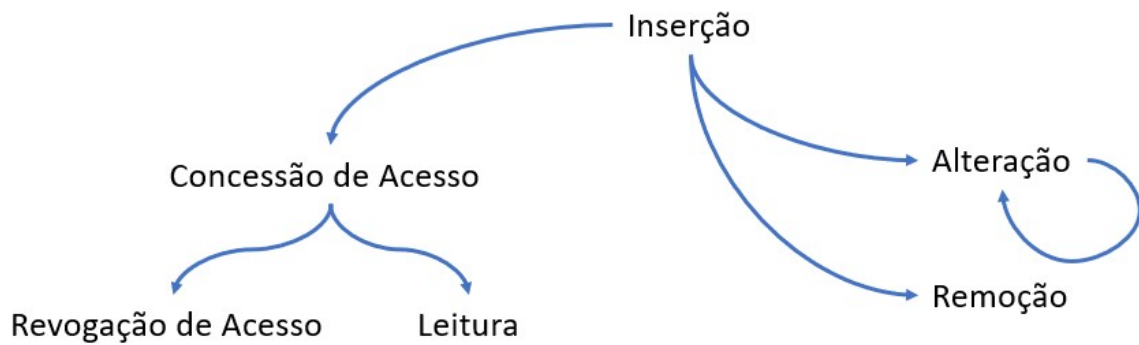


Figura 1 – Diagrama de estados.

A *Personal Blockchain* armazenaram todos os dados que o usuário quiser gerenciar em seus domínios e os eventos que ocorrerem com esses dados. Os dados terão seu ciclo de vida registrado na *blockchain* interna, assim como o próprio dado. As deleções e retificações serão realizadas de forma lógica, ou seja, para uma deleção os registros não serão fisicamente excluídos, apenas não estarão mais disponíveis para consulta; já para os dados retificados, apenas estará disponível sua última versão. Mesmo com retificações e deleções lógicas, os dados estarem armazenados internamente ao ambiente do dono dos dados, dessa maneira, a ação lógica não fere os princípios legais trabalhados nesse trabalho. A estratégia também prevê um processamento restrito das informações, apenas o usuário da *Personal Blockchain* e o solicitante processam os dados, minificando a quantidade de processamento dos dados.

Além disso, todo estado ocorrido no ciclo de vida do dado (vide Figura 1) é registrado na *Personal Blockchain*, assim, torna possível a entidade que recebeu os dados compartilhados e o dono dos dados se defender contra acusações de adulteração de dados, pois a *Personal Blockchain* se utiliza de uma *blockchain* externa ancorando os dados internos.

- os blocos, identificados com a letra “I”, guardam as informações inseridas na blockchain.
- os blocos auxiliares, identificados com a letra “A”, são responsáveis por dificultar a recriação maliciosa da cadeia;
- os blocos de eixo, identificados pela letra “E”, são blocos que apoiam os blocos auxiliares para dificultar a recriação da cadeia, mas tem como função principal ancorar a *blockchain* matricial à *blockchain* externa. Os blocos de eixo não fazem parte fisicamente da *blockchain* matricial, a ligação é apenas lógica, servindo para possibilitar a auditoria nos blocos internos.
- o bloco raiz, identificado pela letra “R”, tem o mesmo objetivo que em *blockchains* tradicionais.

É importante perceber que a estrutura da *blockchain* tradicional ainda está presente no núcleo da *blockchain* matricial representado pelos blocos de informação e o bloco raiz. Levando em consideração que as setas informam a dependência para a criação do hash único de cada bloco, pode-se dizer que a estrutura da *blockchain* tradicional está preservada, pois seus blocos membros não dependem de blocos extras da nova apresentação.

4.1.2 Blockchain Externa ou Âncora

A *blockchain* externa é uma estrutura de apoio agregada no sistema para prover uma maior segurança ao sistema. O modelo de âncora com *blockchains* pode ser visto em outros artigos como em Weber et al. (2019), porém com um enfoque um pouco diferente do utilizado neste trabalho. O modelo de âncora é a utilização de uma *blockchain* secundária para registrar informações, como o hash, de um bloco que pertence a *blockchain* principal. Dessa forma, tornando mais difícil a adulteração dos dados da *blockchain* principal. Para a arquitetura de rede individual com âncora, a utilização de uma *blockchain* para ancorar a *blockchain* matricial tem como objetivo gerar mais segurança para os registros inseridos na *blockchain* interna, trazendo irretratabilidade e possibilidade de auditoria nos dados.

A transferência de dados entre dois nós em um sistema distribuído tem como ponto fundamental a confiança entre os participantes, possibilitar o rastreo de todo o ciclo de vida das informações registradas é essencial para possibilitar essa confiança. Nesse ponto, a *blockchain* externa é um essencial complemento a *blockchain* interna, devido a vulnerabilidade da interna ter apenas um único contribuinte e guardião, além de possibilitar a utilização de uma cadeia curta para armazenamento de dados.

Todas as informações inseridas na *blockchain* interna e os blocos gerados nessa inserção tem seu hash gravado direta ou indiretamente na *blockchain* externa. Por mais que seja utilizado o termo "rede individual", ele só diz respeito a *blockchain* interna, pois a *blockchain* âncora deve ancorar diversas *blockchains* matriciais. O termo "deve" empregado anteriormente reforça a necessidade de ter várias *blockchains* matriciais ancoradas a uma

blockchain externa ou que seja uma *blockchain* pública com numerosos registros, dessa forma dando maior robustez ao sistema.

Sendo assim, como todos os blocos estão ligados de forma direta ou indiretamente aos blocos da *blockchain* externa, a partir da *blockchain* externa é possível validar qualquer bloco da *blockchain* interna.

4.1.3 Modelo Estrutural Interno

O modelo estrutural interno define como é montada a *blockchain* matricial com âncora. Como pode ser visto na Figura 2, como já mencionado, existem 4 tipos de blocos: os blocos identificados com a letra “I” guardam as informações inseridas na carteira digital e o ciclo de vida dessas informações; os blocos auxiliares, identificados com a letra “A”, responsáveis por dificultar a recriação maliciosa da cadeia; os blocos de eixo, identificados pela letra “E”, são blocos que apoiam os blocos auxiliares para dificultar a recriação da cadeia, mas tem como função principal ancorar a *blockchain* à *blockchain* pública; e o bloco raiz, identificado pela letra “R”. No Algoritmo 1 é possível evidenciar a lógica de implementação utilizada para criar uma *Personal Blockchain* utilizando a arquitetura da *blockchain* matricial com âncora .

Algoritmo 1 Algoritmo de criação de blocos da *blockchain* matricial com âncora.

Exige: *informacao* $\neq 0$

```

blocoInformação  $\leftarrow$  gerarBlocoI(informação)
últimoDireita  $\leftarrow$  gerarBlocoA(blocoInformação)
últimoEsquerda  $\leftarrow$  gerarBlocoA(blocoInformação)
anchorGenerate(últimoDireita)
anchorGenerate(últimoEsquerda)

```

Outro ponto do modelo físico é a arquitetura física de comunicação que detalha a interação entre as diferentes partes que compõem o sistema distribuído. Existem três partes: *blockchain* interna, a *blockchain* âncora e o sistema do requerente das informações, o cliente.

Na Figura 3, pode ser visto o modelo geral de funcionamento e, também, todas as fachadas de serviços baseados nos contratos.

4.1.4 Contratos de Serviços

Toda comunicação entre atores na arquitetura é realizada por meio de implementações de seus contratos. A seguir serão apresentados os contratos que devem ser seguidos para a comunicação ser realizada. Ressalta-se que o modelo apresentado levou em conta a utilização do cenário de comunicação via internet, ou seja, respeitando a pilha TCP/IP, utilizando HTTPs e comunicação via RESTful. Também, será indicado os códigos de status

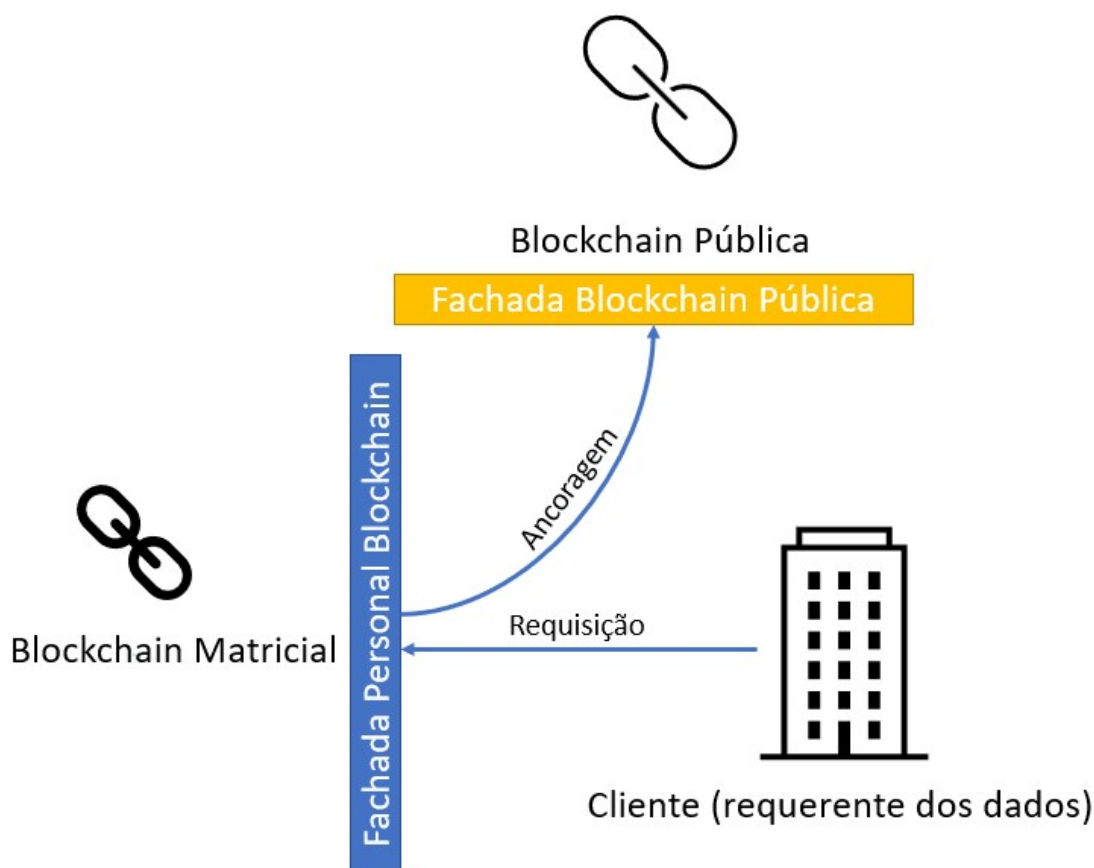


Figura 3 – Arquitetura física de comunicação.

de respostas HTTP que serão retornados seguindo a RFC 2616 e RFC 7231 (CÓDIGOS..., 2022).

Os métodos presentes no contrato da API são:

- *insert*: método utilizado pelo dono da *Personal Blockchain* para inserir novas informações. Ao realizar a inserção, o dado é registrado na *blockchain* matricial com âncora e será retornado HTTP 201. Caso o usuário tente inserir dois dados com o mesmo identificador, não será armazenado o segundo e o método retornará erro HTTP 400.
- *update*: método utilizado pelo dono da *Personal Blockchain* para atualizar uma informação já inserida anteriormente. A informação é registrada como um novo bloco de informação na *blockchain* matricial com âncora. Será retornado HTTP 200. Se não houver registro com identificador informado, será retornado HTTP 400.
- *remove*: método utilizado pelo dono da *Personal Blockchain* para remover uma informação já inserida anteriormente. A informação de remoção é registrada como uma nova informação na *blockchain* matricial com âncora. Quando a operação for realizada com êxito retornará HTTP 200, caso não, retornará HTTP 400.
- *read*: método utilizado pelo cliente para ler os dados que tem acesso na *Personal*

Blockchain. Os dados são lidos um de cada vez e para cada requisição é verificado se o requisitante tem permissão para acessar o dado solicitado. Caso não tenha permissão, será retornado HTTP 403. Caso não exista o identificador informado, será retornado HTTP 400. Caso o identificador seja localizado e o cliente tenha permissão, será retornado HTTP 200 junto com a informação no corpo da resposta.

- *consent*: método utilizado pelo cliente para solicitar consentimento de utilização de um dado. Após realizado essa requisição, o dono da carteira poderá aceitar ou não compartilhar o dado. Caso a resposta seja negativa ou o dado não exista na carteira, o retorno será HTTP 400. Caso seja positiva, o retorno será HTTP 200 e no corpo do pacote terá um identificador único do cliente. O identificador deverá ser utilizado para se identificar quando for necessário utilizar o método *read*.
- *revoke*: método utilizado pelo dono da *Personal Blockchain* para revogar, parcialmente ou totalmente, o acesso a dados compartilhados, retorna HTTP 200 caso haja o registro do cliente e HTTP 400 caso não.
- *getConsents* e *getHistory*: são métodos utilizados pelo dono da carteira de dados para identificar as permissões atualmente concedidas e o histórico de algum dado em específico. O retorno padrão é HTTP 200. Caso o identificador do dado não seja encontrado, retorna HTTP 400.

Todos os métodos apresentados, quando acionados, registram seu acionamento e modificações realizadas na *blockchain* matricial com âncora.

A fachada da *blockchain* pública externa indicada na Figura 3 só apresenta um único método o *anchorGenerate*. Esse método tem a função de criar um bloco na *blockchain* pública que servirá de âncora para a *blockchain* interna.

O cliente não necessitará de uma padrão, apenas deve se atentar que os dados obtidos não devem ser armazenados em seus domínios, se não forem estritamente necessários. Caso os dados sejam armazenados, fica a cargo do cliente consultar os dados na API periodicamente para apagar ou modificar os dados, quando necessário.

5 Cenários de Uso

Para demonstrar a viabilidade do conceito proposta, são apresentados cenários de uso que abrangem as principais situações encontradas no uso da *Personal Blockchain* para armazenamento de informações do usuário e para o gerenciamento do consentimento do usuário, incluindo o direito de esquecimento e o direito de retificação.

De forma geral, os cenários iniciam a interação com o cliente (o requisitante) solicitando o endereço da API da *blockchain* pessoal. O usuário da *Personal Blockchain* fornecerá o endereço. Em posse do endereço, o cliente poderá iniciar a o processo de solicitação e obtenção dos dados. A Figura 4 demonstra o processo de obtenção de consentimento.

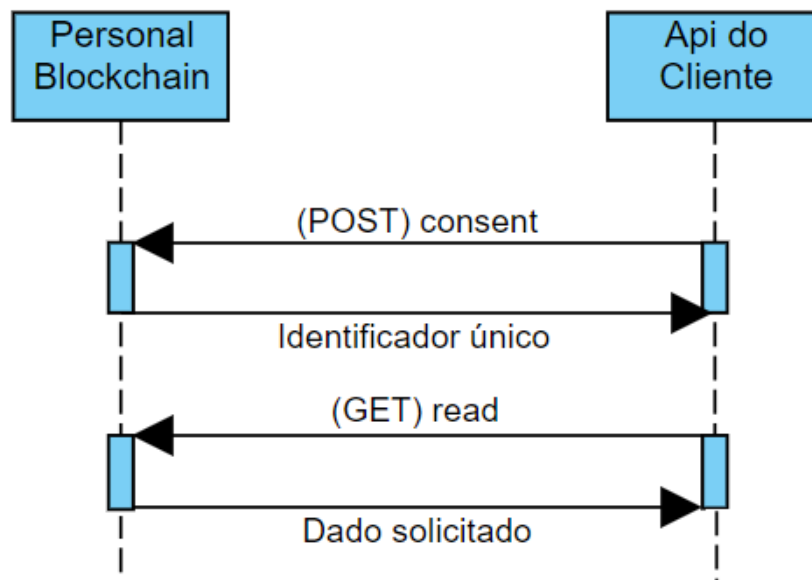


Figura 4 – Diagrama de sequência de concessão do consentimento e atualização de dados.

Após o consentimento ter sido dado, o cliente poderá solicitar o dado em si. Ao solicitar o dado, a *Personal Blockchain* informa o último valor daquele dado para o cliente. Com a posse da informação, o cliente poderá armazená-la em sua base de dados ou não, porém a fonte primária dos dados é a *Personal Blockchain* e todas as alterações de dados e de consentimento estarão registradas na *Personal Blockchain* e ancoradas na *blockchain* pública. Caso o cliente decida armazenar os dados em seus domínios, ele precisará periodicamente consultar a API da *Personal Blockchain* para verificar se houve alguma modificação no dado ou na concessão do acesso.

O usuário, a qualquer tempo, pode alterar ou inserir novos dados na carteira. Também poderá remover dados ou revogar acessos de clientes, como mostrado na Figura 5.

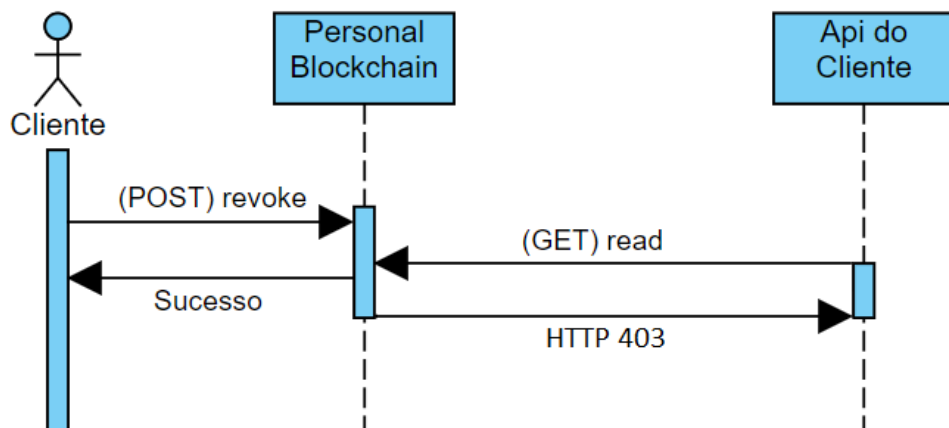


Figura 5 – Diagrama de sequência de concessão da remoção e revogação.

Nesse ponto, acontece a inversão da lógica de responsabilidades dos sistemas tradicionais, aqui, o requerente dos dados é quem tem que verificar se ainda tem as concessões de utilização dos dados, não o dono dos dados que tem a obrigação de informar aos clientes.

5.1 Caso exemplo: Concessão de dados

O usuário deseja fazer uma compra na empresa XPTO S.A., mas não tem cadastro nela.

O usuário informa o endereço da sua *Personal Blockchain*. Com posse do endereço, a empresa solicita via API o acesso aos dados, o usuário concede o acesso aos dados. Ao receber resposta positiva, a empresa solicita os dados à carteira de dados pessoais. Após realizada a leitura, o usuário consegue realizar suas compras com o cadastro já realizado, sem necessitar preencher um cadastro manualmente.

5.2 Caso exemplo: Retificação de dados

Meses depois da primeira compra, o usuário decide novamente realizar uma compra na empresa XPTO S.A. Porém, durante os meses anteriores, ele havia se mudado e atualizado o endereço na *Personal Blockchain*.

Ao realizar a compra, o sistema da XPTO S.A. traz a informação do endereço atualizada, pois já havia atualizado os dados. Com os dados corretos, a compra é finalizada.

5.3 Caso Exemplo: Solicitação de Esquecimento

Pouco tempo após a segunda compra, o usuário considera que não quer mais ter vínculo com a empresa XPTO S.A.

Por meio da aplicação da *Personal Blockchain*, ele revoga as permissões. Periodicamente, a empresa XPTO S.A. verifica se houve alguma modificação nos dados ou nos acessos dos dados presentes na *Personal Blockchain*, quando identifica que o acesso foi revogado, a empresa faz a exclusão dos dados necessários.

5.4 Caso Exemplo: Auditoria

Alguns meses depois, órgãos de controle decidem fiscalizar a empresa XPTO S.A. sobre o cumprimento das leis de proteção de dados vigentes. Durante o processo, identifica que existem dados do usuário registrados na base de dados da empresa. Para se certificar que os dados realmente tinham sido autorizados, o órgão solicita a *Personal Blockchain* do usuário. Os dados da carteira são validados com suas últimas ancoras geradas. Após a validação, é identificado que o usuário realmente havia concedido os dados, porém já havia retirado a concessão.

6 Benchmark e Comparação

Foi implementado algoritmos para a *blockchain* tradicional (controle) e para a *Personal Blockchain*, implementada utilizando a *blockchain* matricial com âncora. O algoritmo da *Personal Blockchain* foi dividido em duas partes por uma separação lógica: a primeira parte é o algoritmo de criação da *blockchain* matricial; já a segunda parte, executada pela primeira, é a implementação para a criação de uma *blockchain* tradicional, ou seja, a *blockchain* que ancora a matricial. Os algoritmos utilizados para as *blockchains* tradicionais foram os mesmos, com a única diferença de que no caso da âncora, ela é iniciada pelo algoritmo da *Personal Blockchain* e não diretamente.

Foram feitos benchmarks entre as duas arquiteturas comparando a estrutura da *blockchain* matricial com âncora com a estrutura tradicional. O intuito do benchmark é comparar o tempo de inserção de blocos de informação na *blockchain* matricial com âncora com o tempo de inserção em uma *blockchain* tradicional. Ou seja, identificar o impacto da inserção dos blocos na estrutura da *blockchain* matricial.

Foram realizados testes de inserção de 3, 30, 300, 3.000 e 30.000 blocos de informação. Todos os testes foram realizados no mesmo computador, nenhum dos testes apresentou gargalo de desempenho por falta de recursos. A máquina utilizada tem um Ryzen 5 quarta geração e 16 Gb de memória RAM. O código foi desenvolvido utilizando linguagem de programação Kotlin. Os resultados estão apresentados na Tabela 1.

Tabela 1 – Tabela de benchmark de execuções de inserção em massa.

Dificuldade	Número de blocos	BMA ^a	BT ^b
Dificuldade 1 zero	3	00h:00min:00s	00h:00min:00s
	30	00h:00min:00s	00h:00min:00s
	300	00h:00min:00s	00h:00min:01s
	30.00	00h:00min:06s	00h:00min:01s
	30.000	00h:10min:45s	00h:00min:01s
Dificuldade 5 zeros	3	00h:00min:07s	00h:00min:08s
	30	00h:00min:37s	00h:00min:40s
	300	00h:07min:15s	00h:06min:24s
	3.000	01h:14min:36s	01h:04min:30s
	30.000	13h:03min:19s	10h:00min:54s

^a*Blockchain* Matricial com Âncora.

^b*Blockchain* Tradicional.

Os testes envolveram a variação de dois parâmetros: a quantidade de blocos inseridos e o número de zeros a esquerda na obtenção dos *hashes* dos blocos das cadeias tradicionais

(ALBUQUERQUE; CALLADO, 2015), ou seja, variação na dificuldade da mineração dos blocos.

Na Tabela 1, é apresentado um benchmark comparativo entre os dois tipos de *blockchain*, é informado o número de blocos de inserção, o tempo decorrido para finalização do processo de inserção e a dificuldade da mineração pelo número de zeros a esquerda que o *hash* deve ter.

Ao analisar a Tabela 1, pode-se evidenciar que, com a mineração facilitada, o tempo de inserção para a *blockchain* matricial com âncora é bem maior comparada a *blockchain* tradicional, porém considerada ainda como viável. O tempo médio de inserção, no caso de 30.000 blocos, é entorno de 2ms. No outro segmento da tabela, com mineração dificultada com 5 zeros, é possível identificar que a diferença relativa diminui em todos os testes, chegando a *blockchain* matricial com âncora, no caso de 30 inserções, ter resultado melhor que a *blockchain* tradicional. Essa queda na supremacia da *blockchain* tradicional evidencia o custo computacional da mineração dos blocos, quão mais difícil for a mineração, menor será a diferença relativa entre as duas *blockchains*. Levando em consideração, que em redes de *blockchains* públicas como Ethereum e o próprio Bitcoin, o número de zeros a esquerda que limita o número de *shes* pode chegar a algumas dezenas de zeros, pode ser afirmado que, se empregado com redes públicas, o tempo de inserção do bloco na *blockchain* interna fica cada vez menos expressivo.

Ainda para corroborar com a análise anterior, pode ser visto nos gráficos da Figura 6 e 7 que mesmo com um tempo médio ponderado bem menor, no caso da *blockchain* tradicional, é possível ver que a maior concentração de blocos inseridos na *blockchain* matricial com âncora leva menos de 2 segundos para a inserção, o que pode ser considerado viável, visto que a *blockchain* tradicional tem tempo médio não ponderado de 1,2 segundos.

O último ponto analisado no benchmark foi o tempo de inserção dos últimos blocos nos testes de 30.000 inserções com 5 zeros, teoricamente, o pior caso para a *blockchain* matricial com âncora, pois é o que exige criação de mais blocos para uma única inserção. Contudo, os últimos blocos que foram inseridos, nos dois casos, levaram 132 milissegundos para sua inserção, na *blockchain* matricial com âncora, e 361 milissegundos, na *blockchain* tradicional. Dessa forma, pode ser evidenciado que o fator “sorte” no acerto do hash da mineração é um fator muito relevante. No melhor caso, o primeiro bloco a ser inserido, os tempos foram 2207ms para a *blockchain* matricial com âncora e 369ms para a tradicional.

A conclusão que pode-se ter é que o *overheading* gerado pela *blockchain* matricial com âncora pode ser compensado por uma heurística mais assertiva na mineração de dados, pois o impacto da mineração de dados no tempo de execução dos algoritmos é muito mais relevante que o *overheading* gerado pela *blockchain* matricial.

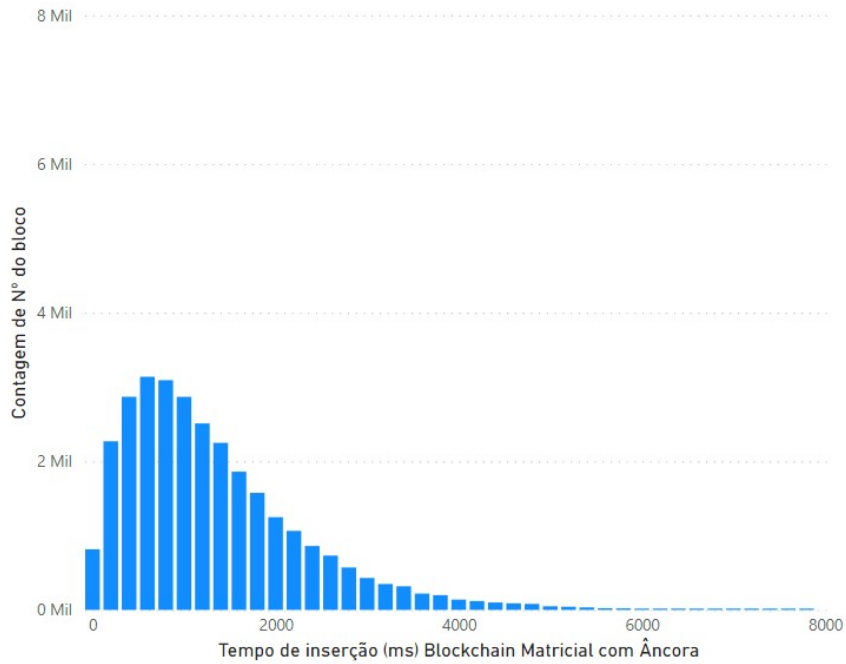


Figura 6 – Gráfico da distribuição de blocos por tempo de inserção na *blockchain* matricial com âncora no teste de 30.000 blocos com dificuldade de 5 zeros.

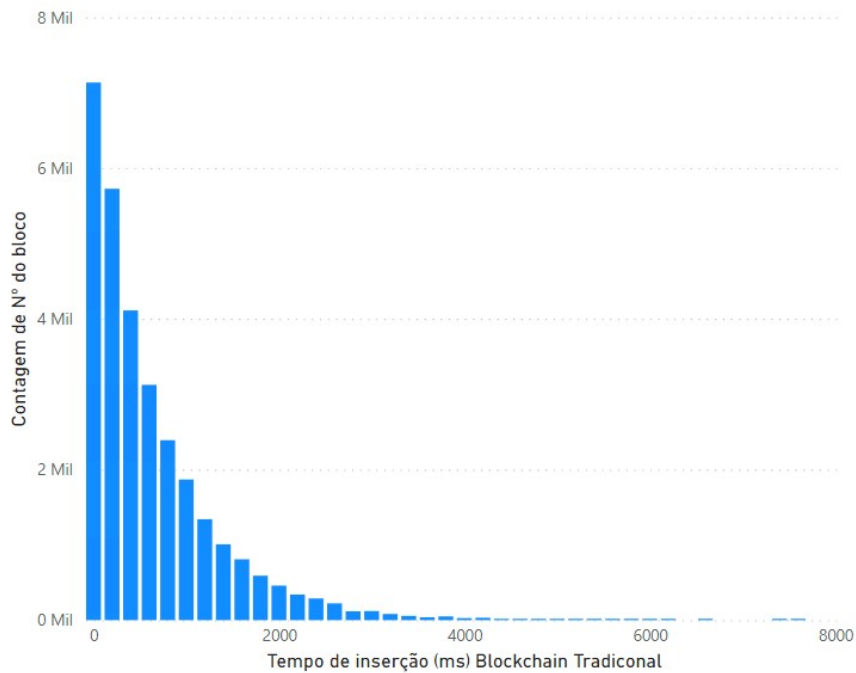


Figura 7 – Gráfico da distribuição de blocos por tempo de inserção na *blockchain* tradicional no teste de 30.000 blocos com dificuldade de 5 zeros.

7 Conclusão

O trabalho traz uma nova estratégia para o armazenamento e compartilhamento de dados com aderência a princípios das leis de proteção de dados. Para possibilitar a implementação da *Personal Blockchain*, foi desenvolvido uma arquitetura baseada em blockchains curtas, a *blockchain* matricial com âncora. Tal arquitetura expande a estrutura arquitetural das *blockchains* tradicionais dimensionalizando a estrutura linear das *blockchains* atuais, assim, criando um modelo de *blockchain* matricial.

O desenvolvimento de uma novo modelo arquitetural de sistema distribuído para propiciar o desenvolvimento da *Personal Blockchain*, teve como ponto central o empoderamento do usuário gerador de dados frente ao requisitantes dos dados, em muitos casos, grandes conglomerados de empresas tecnológicas que tem a posse, a guarda e executam todas as ações em cima do dados.

Também, foram realizadas análises sobre o funcionamento prático da *Personal Blockchain*. *Benchmarks* e validações foram utilizados para testar o uso do conceito em cenários que permitam um fluxo completo do ciclo de vida dos dados. O *benchmark* foi realizado com uma implementação da *Personal Blockchain* baseada na arquitetura da *blockchain* matricial com âncora.

A partir das análises realizadas, foi possível identificar que a abordagem proposta possibilita que uma *blockchain* curta tenha uma robustez maior do que uma *blockchain* tradicional de tamanho similar. O auxílio de uma estrutura de âncora apoia a resiliência da *blockchain* matricial, tornando-a mais confiável e auditável, duas das principais características das *blockchains* tradicionais. Como demonstrado pelos *benchmarks* apresentados, a estrutura matricial não implica em um *overheading* expressivo em comparação com o grande gasto computacional requerido para a mineração dos dados nas cadeias de grande volume.

Além dos ganhos técnicos, o trabalho também abre uma discussão sobre o domínio dos dados e a responsabilidade do uso. Os dados sensíveis de um usuário estão sob sua esfera de controle e devem ser submetidos a seu crivo, como consagram as novas legislações de proteção de dados. Com as soluções existentes hoje, o usuário apenas é um gerador de informações, toda a guarda e manipulação é feita pelos requisitantes dos dados. Faz-se necessário a comunidade científica se debruçar sobre esse novo paradigma de domínio dos dados, até que ponto é possível consentir sobre um uso de dados que o usuário não tem a posse ou que não tenha uma forma tecnológica transparente de cobrar os requisitantes dos dados. Nesse projeto, é esboçado um avanço sobre a possibilidade dos usuários terem o domínio de seus dados, serem eles próprios os guardiões dos seus dados.

Os próximos passos serão o estudo sobre a monetização da mineração da cadeia externa para possibilitar o uso de *blockchains* públicos, estudo sobre os aspectos de segurança da *Personal Blockchain*, o desenvolvimento de aplicações com a arquitetura e o desenvolvimento de arquiteturas com dimensionalidade variável.

Referências

AEPD, A. E. de Protección de D. *JUDGMENT OF THE COURT (Grand Chamber)*. 2014. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62012CJ0131>>. Citado na página 30.

AHMED, J. et al. GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach. In: *2020 3rd International Conference on Information and Computer Technologies (ICICT)*. San Jose, CA, USA: IEEE, 2020. p. 307–312. ISBN 978-1-72817-283-5. Disponível em: <<https://ieeexplore.ieee.org/document/9092226/>>. Citado 2 vezes nas páginas 24 e 30.

AL-ZABEN, N. et al. General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management. In: *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. Southend, United Kingdom: IEEE, 2018. p. 77–82. ISBN 978-1-5386-4904-6. Disponível em: <<https://ieeexplore.ieee.org/document/8658586/>>. Citado 4 vezes nas páginas 23, 25, 35 e 36.

ALBUQUERQUE, B. S. d.; CALLADO, M. d. C. Understanding Bitcoins: Facts and Questions. *Revista Brasileira de Economia*, v. 69, n. 1, 2015. ISSN 0034-7140. Disponível em: <<http://www.gnresearch.org/doi/10.5935/0034-7140.20150001>>. Citado na página 48.

ANTONPOULOS, A. M. Consensus attacks. In: MCGOVERN, T. (Ed.). *Mastering Bitcoin: Programming the Open Blockchain*. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc., 2017. Citado na página 32.

BAYLE, A. et al. When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. In: *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*. Santiago: IEEE, 2018. p. 788–792. ISBN 978-1-5386-7325-6. Disponível em: <<https://ieeexplore.ieee.org/document/8609693/>>. Citado na página 35.

BRASIL. *Lei Geral de proteção de Dados Pessoais (LGPD)*. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Citado 4 vezes nas páginas 23, 29, 30 e 31.

CASINO, F. et al. Immutability and Decentralized Storage: An Analysis of Emerging Threats. *IEEE Access*, v. 8, p. 4737–4744, 2020. ISSN 2169-3536. Disponível em: <<https://ieeexplore.ieee.org/document/8941045/>>. Citado na página 25.

CÓDIGOS de status de respostas HTTP. 2022. Disponível em: <<https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status>>. Citado na página 41.

HAQUE, A. B. et al. GDPR Compliant Blockchains – A Systematic Literature Review. *IEEE Access*, p. 1–1, 2021. ISSN 2169-3536. Disponível em: <<https://ieeexplore.ieee.org/document/9389714/>>. Citado 4 vezes nas páginas 23, 26, 31 e 35.

HERIAN, R. Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, v. 12, n. 1, p. 156–174, jan. 2020. ISSN 1757-9961, 1757-997X. Disponível em:

<<https://www.tandfonline.com/doi/full/10.1080/17579961.2020.1727094>>. Citado 2 vezes nas páginas 25 e 36.

HJERPPE, K.; RUOHONEN, J.; LEPPÄNEN, V. Annotation-Based Static Analysis for Personal Data Protection. In: FRIEDEWALD, M. et al. (Ed.). *Privacy and Identity Management. Data for Better Living: AI and Privacy*. Cham: Springer International Publishing, 2020. v. 576, p. 343–358. ISBN 978-3-030-42503-6 978-3-030-42504-3. Series Title: IFIP Advances in Information and Communication Technology. Disponível em: <http://link.springer.com/10.1007/978-3-030-42504-3_22>. Citado na página 29.

HUANG, H. et al. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools. *ACM Computing Surveys*, v. 54, n. 2, p. 1–42, abr. 2021. ISSN 0360-0300, 1557-7341. Number: 2. Disponível em: <<https://dl.acm.org/doi/10.1145/3441692>>. Citado na página 35.

HUANG, W.-C.; YEH, L.-Y.; HUANG, J.-L. A Monitorable Peer-to-Peer File Sharing Mechanism. In: *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. Matsue, Japan: IEEE, 2019. p. 1–4. ISBN 978-4-88552-320-5. Disponível em: <<https://ieeexplore.ieee.org/document/8892963/>>. Citado 2 vezes nas páginas 25 e 36.

KADENA, E.; HOLICZA, P. Security Issues in the Blockchain(ed) World. In: *2018 IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI)*. Budapest, Hungary: IEEE, 2018. p. 000211–000216. ISBN 978-1-72811-117-9. Disponível em: <<https://ieeexplore.ieee.org/document/8928212/>>. Citado na página 35.

KAKARLAPUDI, P. V.; MAHMOUD, Q. H. A Systematic Review of Blockchain for Consent Management. *Healthcare*, v. 9, n. 2, p. 137, fev. 2021. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute. Disponível em: <<https://www.mdpi.com/2227-9032/9/2/137>>. Citado 2 vezes nas páginas 25 e 26.

LEE, N.-Y. et al. Modifiable Public Blockchains Using Truncated Hashing and Sidechains. *IEEE Access*, v. 7, p. 173571–173582, 2019. ISSN 2169-3536. Disponível em: <<https://ieeexplore.ieee.org/document/8917564/>>. Citado 4 vezes nas páginas 23, 26, 31 e 36.

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Citado na página 31.

OBSERVATORY, T. E. U. B.; FORUM. *Blockchain and the GDPR*. 2018. Disponível em: <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf>. Citado na página 24.

PARLIAMENT, E. *Official Journal of the European Union*. 2016. Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>. Citado 4 vezes nas páginas 24, 29, 30 e 31.

POLITOU, E. et al. Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Transactions on Emerging Topics in Computing*, p. 1–1, 2020. ISSN 2168-6750, 2376-4562. Disponível em: <<https://ieeexplore.ieee.org/document/8883080/>>. Citado na página 35.

SAGLAM, R. B. et al. A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR. In: *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. Oxford, United

Kingdom: IEEE, 2020. p. 22–31. ISBN 978-1-72816-978-1. Disponível em: <<https://ieeexplore.ieee.org/document/9126010/>>. Citado 3 vezes nas páginas 24, 25 e 36.

SANDHU, K.; PABLOS, P. Ordóñez de (Ed.). *Digital Transformation and Innovative Services for Business and Learning*. IGI Global, 2020. (Advances in Business Strategy and Competitive Advantage). ISBN 978-1-79985-175-2 978-1-79985-177-6. Disponível em: <<http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-5175-2>>. Citado na página 31.

SIM, W. L.; CHUA, H. N.; TAHIR, M. Blockchain for Identity Management: The Implications to Personal Data Protection. In: *2019 IEEE Conference on Application, Information and Network Security (AINS)*. Pulau Pinang, Malaysia: IEEE, 2019. p. 30–35. ISBN 978-1-72813-306-5. Disponível em: <<https://ieeexplore.ieee.org/document/8968708/>>. Citado 3 vezes nas páginas 23, 25 e 36.

STAN, O. P.; MICLEA, L. New Era for Technology in Healthcare Powered by GDPR and Blockchain. In: VLAD, S.; ROMAN, N. M. (Ed.). *6th International Conference on Advancements of Medicine and Health Care through Technology; 17–20 October 2018, Cluj-Napoca, Romania*. Singapore: Springer Singapore, 2019. v. 71, p. 311–317. ISBN 9789811362064 9789811362071. Series Title: IFMBE Proceedings. Disponível em: <http://link.springer.com/10.1007/978-981-13-6207-1_49>. Citado 2 vezes nas páginas 31 e 35.

TATAR, U.; GOKCE, Y.; NUSSBAUM, B. Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*, v. 38, p. 105454, set. 2020. ISSN 02673649. Disponível em: <<https://linkinghub.elsevier.com/retrieve/pii/S0267364920300595>>. Citado na página 29.

VOIGT, P.; BUSSCHE, A. von dem. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. 1st ed. 2017. ed. Cham: Springer International Publishing : Imprint: Springer, 2017. ISBN 978-3-319-57959-7. Citado na página 23.

WEBER, I. et al. A Platform Architecture for Multi-Tenant Blockchain-Based Systems. In: *2019 IEEE International Conference on Software Architecture (ICSA)*. Hamburg, Germany: IEEE, 2019. p. 101–110. ISBN 978-1-72810-528-4. Disponível em: <<https://ieeexplore.ieee.org/document/8703904/>>. Citado 2 vezes nas páginas 32 e 39.